OPM Cybersecurity Incident Update #4 – 18 June 2015

Point of Contact: HRPolicy@aafes.com

Fellow Associate,

On 16 June 2015, we sent you an update regarding the OPM cybersecurity incident. We also communicated on 15 June 2015 that individuals whose Personally Identifiable Information (PII) was potentially compromised in the incident would receive an email from OPM in the coming weeks.

As of today on 18 June 2015, OPM has updated the notification email. The email will still come from opmcio@csid.com and it will contain information regarding credit monitoring and identity theft protection services being provided to those Federal employees impacted by the data breach. Below is what the updated email looks like.

We will continue to provide updates as more information becomes available. If you have any questions please refer them to the **hrpolicy@aafes.com.**

Modified CSID OPM data theft notification email

Dear TEST MEMBER,

I am writing to inform you that the U.S. Office of Personnel Management (OPM) recently became aware of a cybersecurity incident affecting its systems and data that may have exposed your personal information.

Since the incident was identified, OPM has partnered with the U.S. Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) to determine the impact to Federal personnel. OPM immediately implemented additional security measures and will continue to improve the security of the sensitive information we manage.

You are receiving this notification because we have determined that the data compromised in this incident may have included your personal information, such as your name, Social Security number, date and place of birth, and current or former address. To help ensure your privacy, upon your next login to OPM systems, you may be required to change your password.

OPM takes very seriously its responsibility to protect your information. While we are not aware of any misuse of your information, in order to mitigate the risk of potential fraud and identity theft, we are offering you credit monitoring service and identity theft insurance through CSID, a company that specializes in identity theft protection and fraud resolution. All potentially affected individuals will receive a complimentary subscription to CSID Protector Plus for 18 months. Every affected individual, regardless of whether or not they explicitly take action to enroll, will have $1 million of identity theft insurance and access to full-service identity restoration provided by CSID until 12/7/16.

Your PIN code is: XXXXXXXXXXXX

To access the trusted pages that will facilitate enrollment into this identity protection service, type or paste the following website into your browser: https://www.csid.com/opm.

You will need to use the PIN code provided to enroll in these services. Individuals can also contact CSID with any questions about these free services by calling this toll free number, 844-777-2743 (International callers: call collect at 512-327-0705).

Protector Plus coverage includes:

- Credit Report and Monitoring: Includes a TransUnion® credit report and tri-bureau monitoring for credit inquiries, delinquencies, judgments and liens, bankruptcies, new loans and more
- CyberAgent® Internet Surveillance: Monitors websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information
- Identity Theft Insurance: Reimburses you for certain expenses in the event that your identity is compromised with a $1,000,000 insurance policy
- Court and Public Records Monitoring: Know if your name, date of birth and Social Security number appear in court records for an offense that you did not commit
- Non-Credit Loan Monitoring: Know if your personal information becomes linked to short-term, high-interest payday loans that do not require credit inquiries
- Change of Address Monitoring: Monitor to see if someone has redirected your mail
- Social Security Number Trace: Know if your Social Security number becomes associated with another individual's name or address
- Sex Offender Monitoring: Know if sex offenders reside in your zip code, and ensure that your identity isn't being used fraudulently in the sex offender registry
- Full-Service Identity Restoration: Work with a certified identity theft restoration specialist to restore your ID if you experience any fraud associated with your personal information

These services are offered as a convenience to you. However, nothing in this letter should be construed as OPM or the U.S. Government accepting liability for any of the matters covered by this letter or for any other purpose. Any alleged issues of liability concerning OPM or the United States for the matters covered by this letter or for any other purpose are determined solely in conformance with appropriate Federal law. Please note that these services are offered to the specific addressee of this letter and are not available to anyone other than the individual who received this notification.

We regret this incident. Please be assured that OPM remains deeply committed to protecting the privacy and security of information and has taken appropriate steps to respond to this intrusion. The incident was uncovered as a result of OPM's aggressive effort to update its cybersecurity posture over the past year, including the addition of numerous tools and capabilities to its networks that both help detect and deter a cyber-attack.

Please note that neither OPM nor any company acting on OPM's behalf will contact you to confirm any personal information. If you are contacted by anyone purporting to represent OPM and asking for your personal information, do not provide it.

To learn more and enroll, visit CSID's website at https://www.csid.com/opm.

OPM Cybersecurity Incident: Additional Information

As a reminder, you should follow the below routine precautionary measures to help protect your identity and personal affairs.

Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.

- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax, Experian, and TransUnion – for a total of three reports per year. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website, www.ftc.gov

- Review resources provided on the FTC identity theft website, www.identitytheft.gov. The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call Trans Union at 1-800-680-7289 to place this alert. TransUnion will then notify the other two credit bureaus on your behalf.

Avoid becoming a victim.

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, www.us-cert.gov/ncas/tips/ST04-013).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (www.antiphishing.org).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, www.us-cert.gov/ncas/tips/ST04-007).
- Take advantage of any anti-phishing features offered by your email client and web browser.

Additionally, if you are or have been a Federal employee or contractor and become aware of any contacts or other activity that could raise security concerns, you should immediately contact your security officer or former security officer for further guidance.
You can obtain additional information about steps to avoid identity theft from the following agencies. The FTC also encourages those who discover that their information has been misused to file a complaint with the FTC.

For California Residents:
Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.

For Kentucky Residents:
Office of the Attorney General of Kentucky
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
Telephone: 1-502-696-5300

For Maryland Residents:
Office of the Attorney General of Maryland Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Telephone: 1-888-743-0023

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.identitytheft.gov
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502